Ferencz Gizella

Ügyfélszerzés mindenáron III. – második szakmai idegen nyelven (német)

NSZFI
NEMZETI SZAKKÉPZÉSI ÉS FELNŐTTKÉPZÉSI INTÉZET

A követelménymodul megnevezése:

A telemarketing, telesales tevékenység ellátása idegen nyelven

A követelménymodul száma: 2569-06 A tartalomelem azonosító száma és célcsoportja: SzT-n22-50

Új Magyarország Fejlesztési Terv

KUNDENGEWINNUNG JEDERZEIT III.

DATENBANK-AUFBAU

EREIGNISBESCHREIBUWNG – DIE ARBEITSSITUATION

1. Bild Meine Identität gehört Mir!

Es klingt lächerlich, aber: Ich habe Angst, den Briefkasten zu öffnen. Beinahe täglich flattern mir derzeit Mahnungen und Drohschreiben von Inkassounternehmen ins Haus. "Weil Sie auf die vorbenannten Forderungen noch immer nicht reagiert haben, leiten wir jetzt das Mahnverfahren ein", steht da zum Beispiel. Schulden soll ich gemacht und Waren bezogen haben von Unternehmen, deren Namen ich noch nie gehört habe. Die Sachen wurden an Adressen geliefert, die nie die meinen waren. Dort soll es sogar Menschen geben, die "zweifellos bezeugen können, dass Sie, Johanna Troll, dort gewohnt haben", schreibt mir eine Inkassofirma. Sogar Haftbefehle gibt es gegen mich – und das völlig unverschuldet. Ich bin Opfer eines Identitätsdiebstahls geworden.

Was seither geschieht, hätte Kafka nicht besser beschreiben können. Es war kurz vor Weihnachten, als mein bisheriges Leben endete und sich das erste Inkassounternehmen bei mir meldete. Die Creditreform will rund 200 Euro für eine Warenlieferung der Württembergischen Metallwaren Fabrik (WMF). Das Schreiben hat den Betreff "Mahnung" und eine Kundennummer. WMF? Creditreform? Zunächst glaube ich, es handelt sich um betrügerische Werbepost. Was tun? Nicht reagieren? Nachhaken? Plötzlich bin ich ganz aufgeregt. Schon damals fanden sich mir unbekannte Adressen und eine Forderung einer Inkasso GmbH über 1000 Euro. Ich hatte widersprochen und die Daten als falsch deklariert. Gemäß des Bundendatenschutzgesetzse müssen falsche Daten gelöscht werden. Das hatte die GmbH auch getan – und ich angenommen, dass es sich nur um Schlamperei oder Verwechslung gehandelt hatte. Doch jetzt kriecht eine Ahnung in mir hoch: Datenmissbrauch? Oder habe ich eine kaufsüchtige Namensschwester?

Ich greife zum Telefonhörer. Mir ist es unangenehm, mich bei der Creditreform mit der Kundennummer zu melden, die einem Schuldenfall zugeordnet ist. Also sage ich: "Es handelt sich um eine angebliche Nummer …" Warum sollte ich sagen, dass es meine Kundenummer sei? Es ist nicht meine! Ich werde zur Inkassoabteilung durchgestellt, aber dort ist niemand mehr erreichbar. Ich bin wütend und erreiche doch gar nichts. Ich lege auf.

"Das ist bestimmt ein Versehen. Du musst widersprechen. Das brauchst du nicht zu bezahlen", sagt mein Vater. Jetzt soll ich widersprechen?! Warum? Das ist doch überhaupt nicht mein Business! Ich habe dazu weder Zeit, noch Lust.

Ich schreibe trotzdem einen Brief. Ich erkläre, dass ich die Mahnung mit Verwunderung erhalten habe, aber ich niemals eine Vertragsbeziehung mit dem Unternehmen gehabt oder angestrebt habe. Ich bitte die Firmen, die falsch über mich gespeicherten Daten zu löschen und mir hierüber eine schriftliche Erklärung zuzusenden.

Im Netz finde ich auf der Website eines Anwalts eine Mitteilung des Justizministeriums. Darin heißt es, man solle auf unberechtigte Rechnungen oder Mahnschreiben gar nicht reagieren, aber es sei sinnvoll, dem Absender mitzuteilen, dass man keinen Vertrag geschlossen habe. Reagieren müsse man erst, wenn es sich um einen Mahnbescheid von einem Gericht handele. Ferner steht dort: "Sollten Sie den Eindruck haben, jemand könne Ihren Namen unbefugt benutzt haben, ist es besonders ratsam, sich mit dem Rechnung stellenden Unternehmen in Verbindung zu setzen. (...) In solchen Fällen einer Bestellung unter falscher Namensangabe sollten ebenfalls die Polizei oder Staatsanwaltschaft eingeschaltet werden." Es beruhigt mich nicht sonderlich.

Immerhin habe ich jetzt einen Namen für das, was geschieht: Identitätsdiebstahl.

Wie klaut man die Identität eines Menschen? Hätte ich noch vor wenigen Wochen von dieser Geschichte gehört, ich hätte gesagt: Das ist doch nicht möglich. Doch es ist sogar sehr einfach. Es braucht nur einen Namen und das dazugehörige Geburtsdatum. Daten, die man leicht im Internet findet. Hat man dann noch einen weiteren Anhaltspunkt, beispielsweise den Beruf der Person, kann man sich munter bedienen.

So machten es wohl auch "meine Betrüger", wie ich sie inzwischen nenne. In möglicherweise Hunderten Fällen haben sie unter einer fiktiven E-Mail-Adresse, die sie aus meinem Namen und meinem Geburtsdatum bastelten, Waren bei Versandhäusern auf Rechnung bestellt. Das ist im Netz kein Problem. Die Geschäftspolitik der Onlineshops macht es Betrügern leicht. Sie liefern an irgendwelche Adressen – in dem Vertrauen darauf, dass der Besteller schon bezahlt.

Der Ärger kommt Wochen später, wenn die Zahlung ausfällt. Dann beginnt das Mahnverfahren an den Schuldiger, natürlich unter den bekannten, in der Bestellung angegebenen Daten. Irgendwann, Monate später, kommen die geprellten Unternehmen dahinter, dass die Adressen nicht korrekt sein können. Meist haben die Firmen die ausstehenden Forderungen dann an Inkassounternehmen abgetreten, die so etwas recherchieren. Sie werden fündig, und zwar bei der realen Person.

FACHLICHER INFORMATIONSINHALT

1. Geschichte

Mit der Verbreitung von Computern, die große Datenmengen verarbeiten können, gewinnt Datenschutz immer mehr an Bedeutung. Anfang der 1960er Jahre begann die Geschichte des modernen Datenschutzes–und zwar in den USA.

Die amerikanische Regierung wollte damals eine EDV-Datenbank aufbauen, in der alle amerikanischen Staatsbürger erfasst werden sollten. Dagegen bestanden in der Bevölkerung massive Bedenken, da in den USA traditionell nicht einmal jeder Bürger einen Personalausweis besitzt.

Der Plan der Regierung wurde als schwerer Eingriff in die Privatsphäre empfunden und erschien vielen als unverhältnismäßig. Ergebnis der öffentlichen Diskussion war, dass die Datenbank nicht errichtet und stattdessen der „Privacy Act“ (Privatsphärengesetz) verabschiedet wurde. Allerdings bezog sich dieses Gesetz nur auf Privatpersonen, nicht auf Privatunternehmen. Bis heute gibt es heftige Diskussionen, wie der Datenschutz bei amerikanischen Unternehmen beim Export von Daten von Europa nach den USA gewährleistet werden kann.

Datenschutz bezeichnet den Schutz des Einzelnen vor dem Missbrauch personenbezogener Daten. Der Begriff wurde auch verwendet für Schutz wissenschaftlicher und technischer Daten gegen Verlust oder Veränderung – und Schutz gegen Diebstahl dieser Daten. Heute bezieht sich der Begriff meist auf den Schutz personenbezogener Daten. Bei personenbezogenen Daten wurde er auch für Schutz vor „Verdatung“ verwendet. Im englischen Sprachraum spricht man von "privacy" (Schutz der Privatsphäre) und von „data privacy“ oder „information privacy“ (Datenschutz im engeren Sinne). Im europäischen Rechtsraum wird in der Gesetzgebung auch der Begriff „data protection” verwendet.

Heute wird der Zweck des Datenschutzes darin gesehen, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird. **Datenschutz steht für die Idee, dass jeder Mensch grundsätzlich selbst entscheiden kann, wem wann welche seiner persönlichen Daten zugänglich sein sollen.** Der Datenschutz will den so genannten gläsernen Menschen verhindern.

Die Bedeutung des Datenschutzes ist seit der Entwicklung der Digitaltechnik stetig gestiegen, weil Datenverarbeitung, Datenerfassung, Datenhaltung, Datenweitergabe und Datenanalyse immer einfacher werden. Technische Entwicklungen wie Internet, E-Mail, Mobiltelefonie, Videoüberwachung und elektronische Zahlungsmethoden schaffen neue Möglichkeiten zur Datenerfassung. Interesse an personenbezogenen Informationen haben sowohl staatliche Stellen als auch private Unternehmen. Sicherheitsbehörden möchten beispielsweise durch Rasterfahndung und Telekommunikationsüberwachung die Verbrechensbekämpfung verbessern, Finanzbehörden sind an Banktransaktionen interessiert, um Steuerdelikte aufzudecken. Unternehmen versprechen sich von Mitarbeiterüberwachung (siehe Arbeitnehmerdatenschutz) höhere Effizienz, Kundenprofile sollen beim Marketing einschließlich Preisdifferenzierung helfen und Auskunfteien die Zahlungsfähigkeit der Kunden sicherstellen (siehe Verbraucherdatenschutz, Schufa, Creditreform). Dieser Entwicklung steht eine gewisse Gleichgültigkeit großer Teile der Bevölkerung gegenüber, in deren Augen der Datenschutz keine oder nur geringe praktische Bedeutung hat.

Vor allem durch die weltweite Vernetzung, insbesondere durch das Internet, nehmen die Gefahren hinsichtlich des Schutzes personenbezogener Daten laufend zu („Das Internet vergisst nicht."). Die Verlagerung (z. B. Outsourcing, Offshoring) von IT-Aufgaben in Regionen, in denen deutsche und europäische Gesetze nicht durchsetzbar sind und ausländische Regierungen Zugang zu nicht für sie bestimmte Daten suchen, macht Datenschutz praktisch oft wirkungslos. Datenschützer müssen sich deshalb zunehmend nicht nur mit den grundlegenden Fragen des technischen Datenschutzes (Datensicherheit) sondern besonders mit der effektiven Durchsetzbarkeit von Datenschutz auseinandersetzen, wenn sie Erfolg haben wollen.

Seit 1980 existieren mit den OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data international gültige Richtlinien, welche die Ziele haben, die mitgliedstaatlichen Datenschutzbestimmungen weitreichend zu harmonisieren, einen freien Informationsaustausch zu fördern, ungerechtfertigte Handelshemmnisse zu vermeiden und eine Kluft insbesondere zwischen den europäischen und US-amerikanischen Entwicklungen zu verhindern.

1981 verabschiedete der Europarat mit der Europäischen Datenschutzkonvention eines der ersten internationalen Abkommen zum Datenschutz. Die Europäische Datenschutzkonvention ist bis heute in Kraft, sie hat jedoch lediglich empfehlenden Charakter. Dagegen sind die Datenschutzrichtlinien der Europäischen Union für die Mitgliedstaaten verbindlich und in nationales Recht umzusetzen.

Moderne Firmen-Call-Center haben Zugriff auf alle Kundendaten. Diese Kundendaten muss man regelmäßig überprüfen und mit neuen Informationen ergänzen. Eine Versicherung AG. möchte sein Geschäftskunden Datenbank erweitern. Der Call-Center-Mitarbeiter soll den Datenbank überprüfen und die Kunden anrufen deren Daten mangelhaft sind, oder deren Daten man korrigieren muss. (z.B.: keine Email-Adresse, kein Handy Nummer sind angegeben) Nur mit Hilfe eines Telefonverkaufsleitfadens kann man erfolgreiche Telefonatgespräche führen. Die Frage ist welcher in der Praxis nützliche Aspekt soll das Manuskript enthalten? Welche Normen müssen eingehalten werden?

Laut des **Datenschutzgesetz** dürfen die Unternehmer als Datenerhebungen und -speicherungen für eigene Geschäftszwecke folgendermaßen handeln:

(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

- 1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,
- 2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder
- 3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

Datenschutz

Mit Hilfe eines Telefonsupports kann ein Kundenservice alle Fragen beantworten. Dazu braucht sicht aber jeder Kunde erstens identifizieren z.B.: mit einer temporären PIN, die man über eine Telefontastatur eingeben muss. Dies stellt sicher, dass nur der richtige Anrufer die Auskunft z.B.: zu einem Mitgliedskonto erhalten kann. Darüber hinaus kann man um weitere personbezogenen oder personbeziehbaren Daten bitten.

Die gesetzlichen Voraussetzungen müssen alle Call-Center Mitarbeiter bewusst sein. **Das Bundesdatenschutzgesetz** enthält die folgenden Definitionen:

Personenbezogene Daten: sind Angaben über eine bestimmte oder eine bestimmbare Person. Zu persönlichen Daten zählen Namen, Anschrift, Geburtsdatum, Alter, Adressen und Telefonnummern, Personalausweisnummer, Kreditkartendaten, Kundenvorlieben und sonstige Dinge, die mit ein Mensch als Individuum zu tun hat.

Das *Deutsche Bundesrecht* definiert in § 3 Absatz 1 Bundesdatenschutzgesetz personenbezogene Daten als **„Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person".**

Daten sind *personenbezogen*, wenn sie eindeutig einer bestimmten natürlichen Person zugeordnet sind oder diese Zuordnung zumindest mittelbar erfolgen kann. Im zweiten Fall spricht man auch von *personenbeziehbaren Daten*. Beispiele für personenbezogene Daten:

- Erika Schmidt hat blaue Augen.
- Albert Kerner besitzt einen VW Golf.
- Der erste Kanzler der Bundesrepublik Deutschland war gebürtiger Kölner.

Im ersten Beispiel wird die Angabe hat blaue Augen der Person Erika Schmidt zugeordnet. Die Angabe hat blaue Augen wird dadurch zu einem personenbezogenen Daten. (Im Regelfall wird die Gesamtinformation "Klaus Meier hat blaue Augen" als personenbezogenen Daten zugeordnet.)

Im zweiten Beispiel "besitzt einen VW Golf" ist eine Information der personenbezogenen Daten. Ein personenbezogenes Daten muss also nicht zwangsläufig ein körperliches Merkmal der Person sein. Es genügt ein Bezug zwischen der Person und einer Sache, einer anderen Person, einem Ereignis, einem Sachverhalt.

Im dritten Beispiel ist die Person, auf die sich die Angabe gebürtiger Kölner bezieht, zwar nicht namentlich genannt. Sie ist jedoch bestimmbar, da allgemein bekannt ist, dass Konrad Adenauer der erste Kanzler der Bundesrepublik Deutschland war.

Auch Daten, über die sich ein Personenbezug herstellen lässt, sind als personenbezogene Daten anzusehen (Beispiel: Kfz-Kennzeichen, Kontonummer, Rentenversicherungsnummer, Matrikelnummer), selbst wenn die Zuordnungsinformationen nicht allgemein bekannt sind. Entscheidend ist allein, dass es gelingen kann, die Daten mit vertretbarem Aufwand einer bestimmten Person zuzuordnen.

Besondere Arten **personenbezogener Daten** sind: Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

Öffentliche und nicht-öffentliche Stellen :

- Öffentliche Stellen des Bundes und der Länder sind die: *Behörden*, *die Organe der Rechtspflege* und andere öffentlich-rechtlich organisierte Einrichtungen, der bundesunmittelbaren *Körperschaften*, *Anstalten und Stiftungen* des öffentlichen Rechts sowie deren *Vereinigungen* ungeachtet ihrer Rechtsform, eine *Gemeinde*, ein *Gemeindeverband*. Als öffentliche Stellen gelten die aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht.

- Nicht-öffentliche Stellen sind *natürliche und juristische Personen*, *Gesellschaften* und andere *Personenvereinigungen* des privaten Rechts, soweit sie nicht unter den öffentlichen Stellen fallen. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

Automatisierte Verarbeitung: ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.

Erheben: ist das Beschaffen von Daten über den Betroffenen.

Verarbeiten: ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten.

Nutzen: ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

Anonymisieren: ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

Pseudonymisieren: ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

Verantwortliche Stelle: ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

Empfänger: ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger,

- die an den Betroffenen ausgegeben werden,
- auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und
- bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

Beschäftigte sind:

- Arbeitnehmerinnen und Arbeitnehmer,
- zu ihrer Berufsbildung Beschäftigte,
- Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),
- in anerkannten Werkstätten für behinderte Menschen Beschäftigte,
- nach dem Jugendfreiwilligendienstgesetz Beschäftigte,
- Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist,
- Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

Datenvermeidung und Datensparsamkeit: Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung: Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Einwilligung: ist nur dann wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben. Soweit besondere Arten personenbezogener Daten erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

Datengeheimnis: Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

Rechte des Betroffenen: Die Rechte des Betroffenen auf Auskunft und auf Berichtigung, Löschung oder Sperrung können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

Sind die Daten des Betroffenen automatisiert in der Weise gespeichert, dass mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage festzustellen, welche Stelle die Daten gespeichert hat, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die Stelle, die die Daten gespeichert hat, weiterzuleiten. Der Betroffene ist über die Weiterleitung und jene Stelle zu unterrichten. Die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, können statt des Betroffenen den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unterrichten.

Technische und organisatorische Maßnahmen: Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Auskunft an den Betroffenen: Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

- die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
- die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und
- den Zweck der Speicherung.

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden.

Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er sich an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden kann.

Die Auskunft ist unentgeltlich.

Berichtigung, Löschung und Sperrung von Daten; Widerspruchsrecht

Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird festgestellt, dass personenbezogene Daten, unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in geeigneter Weise festzuhalten.

Personenbezogene Daten, sind zu löschen, wenn

- ihre Speicherung unzulässig ist oder

- ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.
- An die Stelle einer Löschung tritt eine Sperrung, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen, oder Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden.

Anrufung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit: Jedermann kann sich an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden.

Scoring: Zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen darf ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen erhoben oder verwendet werden, wenn

- die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind,
- im Fall der Berechnung des Wahrscheinlichkeitswerts durch eine Auskunftei die Voraussetzungen für eine Übermittlung der genutzten Daten und in allen anderen Fällen die Voraussetzungen einer zulässigen Nutzung der Daten vorliegen,
- für die Berechnung des Wahrscheinlichkeitswerts nicht ausschließlich Anschriftendaten genutzt werden,
- im Fall der Nutzung von Anschriftendaten der Betroffene vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten unterrichtet worden ist;

die Unterrichtung ist zu dokumentieren.

Benachrichtigung des Betroffenen:

1. Werden erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu benachrichtigen.

2. Werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen.

Berichtigung, Löschung und Sperrung von Daten

1. Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Geschätzte Daten sind als solche deutlich zu kennzeichnen.

2. Personenbezogene Daten können jederzeit gelöscht werden. Personenbezogene Daten sind zu löschen, wenn

- ihre Speicherung unzulässig ist,
- es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann,
- sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, oder
- sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden. Personenbezogene Daten, sind nach Beendigung des Vertrages auch zu löschen, wenn der Betroffene dies verlangt.

3. An die Stelle einer Löschung tritt eine Sperrung, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.

2. Bild Kundenkontakt per Telefon

Kunden treten über die unterschiedlichsten Medien mit Unternehmen in Kontakt. Produktanfragen über das www, die Kündigung einer Versicherungspolice per Brief, Anrufe beim Service Center oder eine Email aufgrund einer Adressänderung des Kunden sind Beispiele für die vielfältigen Kundenkontakte, die in heutigen Unternehmen bestehen. In vielen Unternehmen entstanden traditionell Insellösungen für die Bearbeitung der einzelnen Medien.

Moderne Call-Center Lösungen liefern die technologische Basis und den organisatorischen Rahmen für das effiziente Management der Kundenkontakte. Call/ Contact-Center bieten eine umfassende Schnittstelle zwischen den Kunden und dem Unternehmen an. Sie bündeln die technischen Kundenkanäle und liefern die Anbindung der verschiedenen Kanäle an die Informationssysteme und Geschäftsprozesse des Unternehmens. Dieser Arbeitsbericht liefert einen Überblick über die verschiedenen Einsatzgebiete, Technologien und Module eines Contact- Center.

Call/ Contact-Center bieten ein weites Spektrum an Funktionalitäten an, sie fungieren als Integrationsplattform für die verschiedenen Kundenkontakte im Unternehmen. Briefe, Fax, Email, WWW, Telefon, Voice Mail etc. sind Möglichkeiten, über welche ein Kunde mit dem Unternehmen in Kontakt treten kann.

Der Einsatzbereich moderner Call-Center erstreckt sich von einfachen Telefonzentralen, die lediglich die Koordination eingehender und ausgehender Anrufe unternehmen, bis hin zum vollintegrierten Customer Interaction Center, in dem sämtliche Kanäle verknüpft und an die Back-Office Systeme angebunden werden. Mit steigendem Integrationsgrad der unterschiedlichen Komponenten erhöht sich der Nutzen, den die Unternehmen ihren Kunden durch den Einsatz von Multi Channel Management bieten können. Der nachhaltige Nutzen in Form erhöhter Kundenzufriedenheit, verbesserter Kundenbindung und effizienter Bearbeitung von Kundenanfragen entsteht jedoch erst nach einer Integration der verschiedenen Kontaktkanäle.

3. Bild Call-Center Einsatzgebiete Weltweit

Einsatzgebiete von Contact-Center

Szenario 1:

Ein Kunde meldet sich bei dem Call-Center eines Kreditinstitutes. Nach der Identifikation des Kunden über ISDN werden sämtliche Kundeninformationen aus der Kundendatenbank des Unternehmens ausgelesen und ein für den Kunden passender Call-Center Mitarbeiter ausgewählt. Die Daten erscheinen parallel zu der Durchleitung des Anrufes auf dem Bildschirm des Call-Center Agenten. Er begrüßt den Kunden persönlich in seiner Muttersprache und kann ihm sofort Auskunft über Kontostand, Anlageempfehlungen, genehmigte Kredite etc. geben. Im System ist die Historie der einzelnen Kundenkontakte, sei es über Telefon, WWW, Email, Fax oder Brief präzise vermerkt. Nach Beendigung des Telefonats werden die Anrufinformationen direkt in das System gespeist. Der Call-Center Agent erhält die Möglichkeit, weitere Informationen zum Gespräch (Gesprächsprotokoll) einzugeben und die Daten gegebenenfalls an weitere Mitarbeiter weiterzuleiten.

Szenario 2:

Ein Versicherungsunternehmen bietet auf seinen Web-Seiten neben Produktinformationen, Anlageempfehlungen und Tarifberechnungen auch die Möglichkeit zur Online-Schadenentgegennahme an. Auf den verschiedenen Seiten haben die Benutzer die Option, einen Rückruf-Button zu drücken. Nach Angabe des Namens, der Telefonnummer oder der Policennummer (nicht notwendig bei Stammkunden) und der gewünschten Rückrufzeit werden diese Informationen an einen passenden Call-Center Agenten übergeben, der den Kunden zur gewünschten Zeit zurückruft. Da die Position innerhalb der Website, von welcher der Benutzer die Anfrage gestartet hat, ebenfalls übermittelt wurde, ist der Call- Center Mitarbeiter schon hinreichend auf den Problem-Kontext vorbereitet. Hat der Kunde beispielsweise Probleme mit der Online- Eingabe eines Schadenfalles, kann der Call-Center Agent über ein Application Sharing Modul den Browser des Kunden „fernsteuern“ und ihn durch die Anmeldeformulare navigieren.

Szenario 3:

Ein deutscher Online-Buchhändler nimmt Bücherbestellungen über das Internet, Email oder per Telefon entgegen. Um eine vierundzwanzigstündige Erreichbarkeit zu gewährleisten, kooperiert der Buchhändler mit einem Call-Center in den USA, welches die Anrufe nach 19:00 entgegen nimmt. Die Anrufe werden direkt über TCP/IP in die USA weitergeleitet. Dort betreuen deutschsprachige Call-Center Mitarbeiter die Kundenanfragen und geben die Bestellungen direkt in das verteilte Informationssystem des Buchhändlers ein. Kunden bemerken die Umleitung ihres Anrufes nicht. Dem Unternehmen entsteht durch die IP-telephony (Internet Protocol telephony) kein zusätzlicher monetärer Aufwand.

Szenario 4:

Im Contact-Center eines mittelständischen Softwareunternehmens werden eingehende Telefonanrufe, Faxe, Emails und Briefe zentral verwaltet. Die Briefe werden eingescannt und, ebenso wie Emails und Faxe automatisch kategorisiert und aufgrund definierter Regeln über ein Workflowmanagementsystem den entsprechenden Abteilungen bzw. Mitarbeitern weitergeleitet. Das Unternehmen verfügt über eine Unified Messaging Lösung, welche eingehende Nachrichten in verschiedene Medienformate transformiert. Außendienstmitarbeiter können eingegangene Faxe oder Briefe über das Telefon abrufen oder erhalten den Verweis auf eingegangene Telefonanrufe per SMS mitgeteilt.

Zusammenfassung

> Aufgabe des **Kundenmoduls des Call/Contact-Centers** ist, dass die Kundendaten für die Mitarbeiter schnell und effektiv zur Verfügung stehen und während der laufenden Arbeit diese Daten weitgehend automatisch verarbeitet sein können.

> Auf der in Klientanwendung integrierten Oberfläche finden wir schnell und effektiv die gesuchten Kunden praktisch mit Eingabe von beliebigen Daten. Beim Zustandekommen der aktiven Anrufe soll der Contact-Center – soweit es anhand der zur Verfügung stehenden Daten möglich ist – den entsprechenden Kunden automatisch ermitteln.

> Das Klient-System reagiert interaktiv auf die durchgeführten Modifizierungen und auf die eventuell begehenden Fehler und Mängel. In der Meldungszeile wird ein eventuelles Problem oder eine notwendige Zusatzinformation für den Mitarbeiter angezeigt.

> *Wenn z.B. die Daten eines Kunden registriert werden und zur Registrierung (Identifizierung) noch Angaben fehlen, das Programm lässt die Registrierung nicht zu. Sogar beim Ausfüllen der einzelnen Felder kann man den Benutzer warnen.*

> Das Telemarketing integrierte System macht es auch möglich, dass die Daten der potenziellen Kunden oder die in der Anrufliste gespeicherten Daten automatisch in das Kundenregistrationssystem übergeführt werden, auch mit der Ergänzung der gewonnenen Informationen aus den Antworten auf die Marketingsfragen.

> Das System behandelt auch die Historie der Kontaktaufnahme, d.h. bei einem Kundenanruf sieht der Mitarbeiter die detaillierten Daten der früheren Kontakte des Kunden.

> Auf der Kundenanruf-Historieseite kann das Ziel, Ergebnis und sonstige Bemerkungen zu dem Anruf dokumentiert werden. Auch eine wichtige Dienstleistung des Systems ist, dass der Mitarbeiter in der Lage ist, einen Rückruf des Kunden, oder potenziellen Kunden innerhalb des Systems zu einem voreingestellten Zeitpunkt zu initialisieren. Auf dem Terminal des Mitarbeiters erscheinen auch die Informationen, die von dem Initiator des Rückrufes registriert worden sind.

<u>Die unterstützenden Dienstleistungen des in das Komplex Call/Contact-System integrierten Telemarketingmoduls(Teilsystem) bei outbond Telefonkampagnen:</u>

- Empfang von Daten aus äußeren Datenbasen mit verschiedenem Format und verschiedener Konstruktion

- Herstellung von Anruf-Datenbasen aus der inneren Datenbasis mit beliebigen Auswahlkriterien aufgrund der Ergebnisse oder Teilergebnisse von bereits abgeschlossenen oder laufenden Aktionen

- Verwaltung von Anruf-Datenbasen aus hybriden – inneren und äußeren – Quellen

- Planung und Herstellung von Scripts (Manuscripts) für das Telemarketing

- Zusammenstellung von Vertriebsaktivitäten mit Telefonverkauf, die durch zwei Richtungen realisiert werden: mit Hilfe inbound und outbond Telefonie

- Abwicklung, zeitliche Planung und Organisation von Telemarketing-Kampagnen, die Monitorierung, Modifizierung, Unterbrechung und Weiterführung deren während des laufenden Prozesses. Das System ist imstande gleichzeitig auch mehrere Kampagnen zu verwalten

- Organisation, Kontrolle des Arbeitsprozesses der Mitarbeiter

- Analysierung und Auswertung von Telemarketing-Kampagnen auch während und nach dem Prozess

- Verwaltung, Management und Erneuerung von tatsächlichen und potenziellen Kundendatenbasen

- Verwaltung von detaillierter Historie der Kontaktaufnahmen.

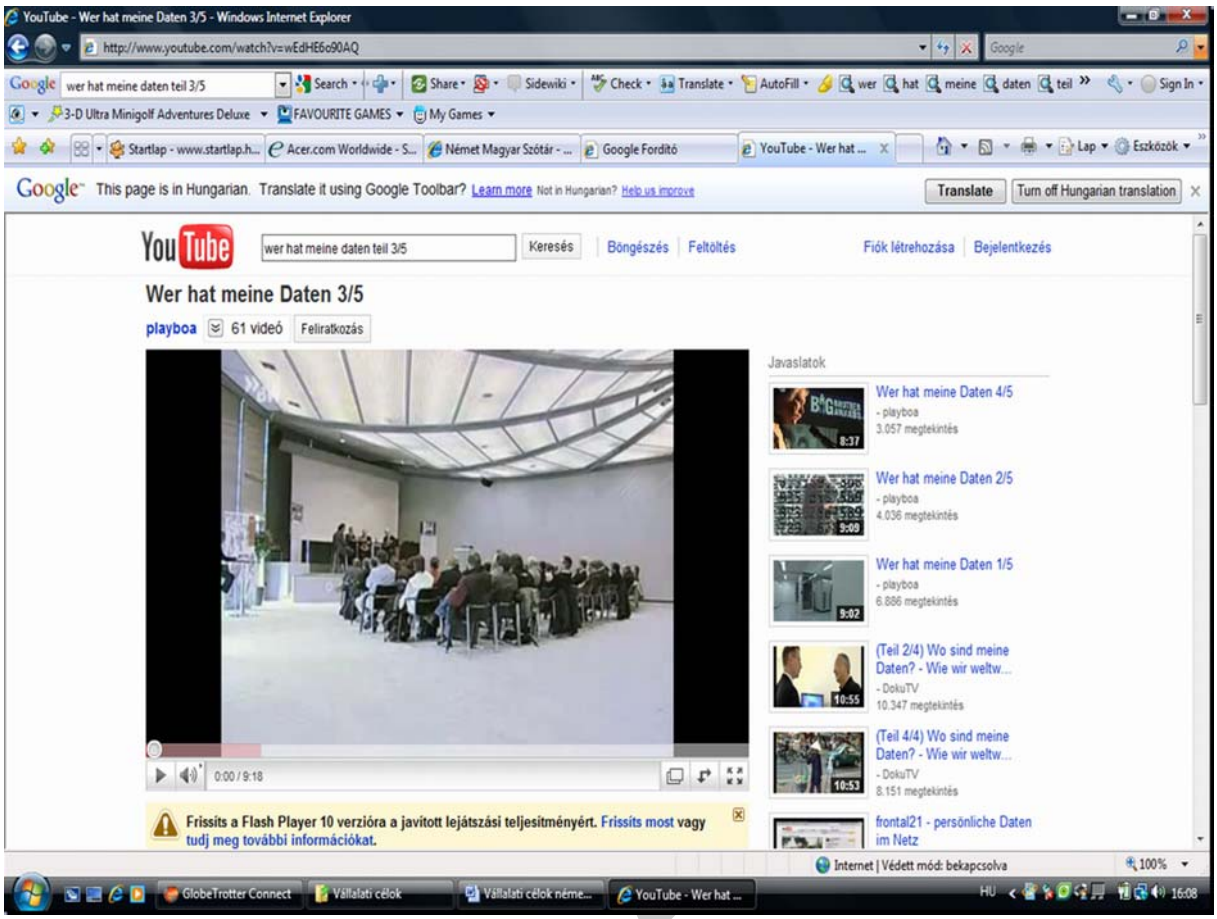
LERNHILFE

Sehen Sie bitte bei den YouTube-Videodarstellungen über den Datenschutz Erich Schütz Reportage an:

1. Aufgabe

Wer hat meine Daten Teil 3/5 (05.09.2010)

Hören Sie die Diskussion an und machen Sie Notize von den Gehörten.



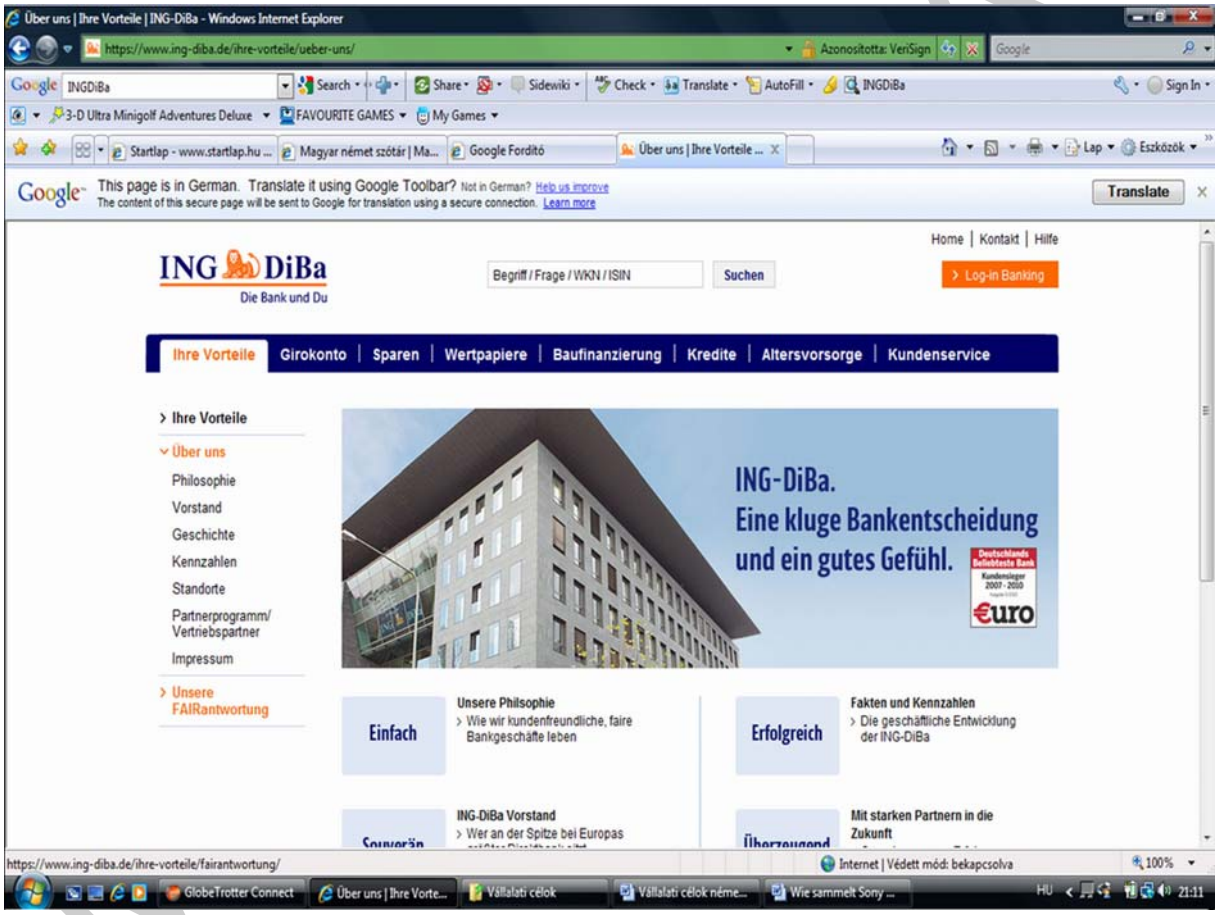
4. Bild "Wer hat meine Daten?"

Erich Schütze berichtet in einem 5 teiligen Reportage über den Datenschutz, Vorteil ist, dass er die Aspekten beider Seiten (Unternehmen + Kunden) berücksichtigt.

SELBSTKONTROLL AUFGABEN

2. Aufgabe

5. Bild ING-DiBa logo



6. Bild ING-DiBa WebSeite

Die ING-DiBa wurde im 2008 zu "Deutschlands beliebtester Bank" gewählt. Zur Philosophie gehört, dass sie transparent ist. Steht für ein besonderes und kundenfreundliches Bankgeschäft. Bietet einfache und transparente Produkte an. Mit einer Tag und Nacht Erreichbarkeit ist Kundennähe gesichert. Sie bieten günstige Zinskonditionen und eine gebührenfreie Kontoführung. Über 7 Millionen Kunden schätzen die ING-DiBa Angebote.

Bitte übersetzen Sie aus dem Deutschen in die Ungarische Sprache die nachfolgenden Datenschutz Hinweise des Unternehmens:

Hinweise zum Datenschutz

Wir freuen uns, dass Sie unsere Webseiten besuchen, und bedanken uns für Ihr Interesse an unserem Unternehmen, unseren Produkten und unseren Webseiten.

Der Schutz Ihrer Privatsphäre bei der Nutzung unserer Webseiten ist uns wichtig. Daher nehmen Sie bitte die nachstehenden Informationen zur Kenntnis:

Allgemeines

Die ING-DiBa AG, im Folgenden "ING-DiBa" genannt, bietet Ihnen mittels Internet diverse Finanzprodukte des Bank- und Versicherungsbereiches an. Darüber hinaus können unsere Kunden zusätzlich die Bereiche Internetbanking + Brokerage erreichen.

Die ING-DiBa ist sich der Bedeutung der ihr anvertrauten personenbezogenen Daten bewusst. Selbstverständlich stellen wir sicher, dass die von Kunden und Interessenten im Rahmen unseres Internet-Angebotes eingegebenen Daten vertraulich behandelt werden.

Personenbezogene Daten sind solche, die Ihrer Person zugeordnet werden können. Darunter fallen z. B. Ihr Name, Ihre Anschrift, Ihre Telefonnummer und weitere für die Geschäftsabwicklung erforderliche Daten. Informationen, die nicht direkt mit Ihrer Person in Verbindung gebracht werden, gehören nicht dazu.

Die personenbezogenen Daten der Kunden und Interessenten werden durch die Anwendung hoher Sicherheitsstandards und durch Arbeitsabläufe, die besonders dazu geschaffen wurden, um den Missbrauch dieser Daten zu verhindern, geschützt.

Erhebung und Verarbeitung personenbezogener Daten

Personenbezogene Daten werden nur erhoben, wenn Sie uns diese von sich aus, zum Beispiel zur Durchführung eines Vertrages oder bei der Registrierung für personalisierte Dienste, mitteilen.

Die Daten werden zur Erbringung der Dienste / Finanzdienstleistungen genutzt. Des Weiteren erhalten Sie, sofern Sie zugestimmt haben, Produktinformationen der ING-DiBa.

Alle persönlichen Daten werden in verschlüsselter Form übertragen, um einem Missbrauch der Daten durch Dritte entgegenzuwirken.

Nutzung und Weitergabe personenbezogener Daten

Die ING-DiBa verarbeitet und nutzt die von Ihnen erhobenen personenbezogenen Daten zur Prüfung und Abwicklung des Vertrages sowie für Zwecke der Werbung oder der Markt- und Meinungsforschung. Sie können jederzeit der Verarbeitung und Nutzung Ihrer personenbezogenen Daten für Zwecke der Werbung sowie der Markt- und Meinungsforschung widersprechen. Es erfolgt keine Weitergabe Ihrer Daten ohne Ihre Einwilligung, es sei denn es besteht eine rechtliche Verpflichtung.

Ihre Rechte

Wir informieren Sie über jede Datenerhebung, soweit personenbezogene Daten betroffen sind. Darüber hinaus erheben, nutzen und verarbeiten wir keine personenbezogenen Daten ohne Ihre ausdrückliche Einwilligung. Sie können jederzeit Ihre Einwilligung widerrufen.

Sind Sie mit der Speicherung Ihrer personenbezogenen Daten nicht mehr einverstanden oder sind die Daten nicht mehr richtig, werden wir – soweit dies nach geltendem Recht zulässig ist – die Löschung oder Sperrung Ihrer Daten veranlassen oder die notwendigen Korrekturen vornehmen.

Wir erteilen Ihnen auf ausdrücklichen Wunsch Auskunft über die personenbezogenen Daten, die wir über Sie gespeichert haben.

Soweit Sie schon Kunde bei der ING-DiBa sind, erfolgen die Datenerhebung, -nutzung und -speicherung im Rahmen des Internetbanking + Brokerage im Rahmen der mit Ihnen abgeschlossenen vertraglichen Vereinbarungen.

Unsere Sicherheitstechnik

Seiten, auf denen wir personenbezogene Daten erheben, sind mit 128 Bit verschlüsselt und durch für die internationale Verschlüsselungszertifizierung zugelassene Einrichtungen zertifiziert.

Für das Internetbanking + Brokerage gelten weitere Sicherheitseinrichtungen (DiBa Key / iTAN-Verfahren).

Unautorisierte Zugänge werden durch ein Firewall-System abgewehrt.

Weitere Informationen entnehmen Sie bitte dem Bereich "Sicherheit", welcher von unserer Homepage aus zu erreichen ist.

Soweit Sie Fragen und Anregungen zum Bereich Datenschutz haben, können Sie uns unter datenschutz@ing-diba.de kontaktieren.

LÖSUNGEN

1. Aufgabe

7. Bild "Wer hat meine Daten?" (2)

Die Videoaufnahme wurde auf der größten Computermesse der Welt aufgenommen. Die Datenschützer haben hier eine Veranstaltung, Thema ist: die Kundenkarte. Wie wertvoll die eigene Daten sind sich, ist es wenigen klar. Der Bundesbeauftragte des Datenschutzes Peter Schaar fordert auf zum bewussten Einsatz der Plastikkarte. " Wichtig ist das ich mir bewusst mache das wenn ich eine Kundenkarte verwende das Geschäft, oder andere die das ausgegeben haben dass die dann auch eine detaillierte Daten über meinem Kaufverhalt speichern kann, bzw. auch wird." Ein juristisches Problem sind für die Datenschützer die Kundenkartendaten wenn die Konzerne es speichern und es mit weiteren Kundendaten verknüpfen. Je mehr Daten im System sind je einfacher kann man sie verknüpfen. Im Deutschland ist es verboten, aber technisch ist es kein Problem. " Die bestimmte Verknüpfungen zwischen unterschiedliche Systems viel leichter geht. Die Kundenkartendaten, die Artikelkennzeichen, die elektronischen Zahlungsmitteln geben die Möglichkeit auf die Person zu beziehen und wenn das mit einer Überwachungskamera kombiniert wird, sind dann relativ viele Kenntnisse bei einem Ladenbesitzer vorhanden."

Im jeden Laden werden die Kunden überwacht, dabei werden meine Daten gesammelt. Es geht nicht nur um den Schutz von Diebstahl sondern auch von dem Einkaufsverhalten den Besucher. Für den Besitzer sind die Personbezogenen Daten wichtig, schon der Kaufmann bei der Ecke merkte sich was Frau Mayer liebt und von welchen Produkt Herr Müller schwärmt, genau dass sind die Daten heute mit dem der Supermarktbesucher zum gläserne Kunde wird.

Thorsten Franz(Happy Digits): wir sind weit entfernt davon gläserne Kunden zum Anschlag zu haben, dabei sind die Informationen die wir in einem solchen Verbundsystem haben akkrediert, zu wenig Einzelkundenbezogen und es gibt Feldern die nicht von unseren Partnerunternehmer abgedeckt werden. "

Die Realität! Mein Warenkorb wird ins Detail erfasst, jeder Artikel wird registriert. Ich bezahle mit einer Karte. Die gekauften Artikel werden gleichzeitig mit meinem Name gespeichert.

Peter Schaar: Wir stellen fest, dass bestimmte Begehrlichkeiten vorhanden sind, in der USA wo es für Privatsektor kaum Datenschutzregelungen gibt ist dort die Verknüpfung über die verschiedenen Daten, wie über das Surfen im Internet, über das Kaufverhalten und andere Daten verbreitet. Wir haben kurz erlebt dass genau diese Daten gestohlen worden sind. Dass heißt dass 100.000 sogar 1.000.000 Daten amerikanischer Kunden in dieser Art und Weise in Hände Dritten landeten und die das schon verwenden um mit einer falschen Identität Produkte zu bestellen. "

Im Innovationszentrum von Metro Group kann man die Datenverarbeitung von Morgen sehen. Der Blick in die Zukunft zeigt zuerst die angenehmen Versuchungen des Unternehmens. In der Zukunft wird einkaufen leicht gemacht wie das demonstriert wurde. Nie mehr wird sonntags Frühstücksei, oder Schoko für die Kinder vergessen. Intelligente Kühlschränke können fehlende Produkte anzeigen. Vom gläsernen Kunden zum gläsernen Kühlschränken. Wenn man ein Produkt aus dem Kühlschrank nimmt, wird im PC eine Liste generiert und es kann mir zeigen welche fehlenden Produkte ich habe. Da kann man eine Einkaufsliste eingeben mit den Mengen. Die Liste kann per E-Mail zum Einkaufsort weitergeleitet werden. Die Liste wird in einem elektronischen Einkaufsberater gespeichert, die nach einer Identifizierung durch den Supermarkt geführt wird. Der Einkaufsberater - ein Mobilkomputer - weiß genau was Zuhause fehlt und wo es im Shop zu finden ist und führt genau zu dem gesuchten Produkt. Natürlich wird alles im Supermarkt registriert was man im Warenkorb einlegt und in der Zukunft soll sich der gesuchte Artikel sich selbst melden. Jedes Produkt ist auf dem Regal mit einem Funkchip ausgerüstet. "Das ist eine Revolution in der Logistik, in Zukunft kann man diese Waren automatisiert registrieren, egal wo sie in der Welt starten vom Produkthersteller, unterwegs im Schiff über die ganze Zeit der Lieferung bekommen wir über Lesergeräte Informationen wo und wann es sich die Ware befunden hat. Das ist mit der Barcode nicht so einfach. " sagt Albrecht von Truchsess (Metro Group).

Statt sichtbaren Barcode, jetzt den unsichtbaren Chip. Noch wird getestet im Metro Group. Kombinierte Etiketten enthalten beide Daten wie Barcode und auch Nutzdaten in einem Chip. Es gibt da drin eine Antenne die dann bei einer Lesergeräte nähe gleich abgelesen wird.

Der Einkaufsberater lässt sich nach dem Einkauf bei der Kasse leicht lesen. Diesen Chip nennt man auch Schnüffelchip, weil er verrät gleich welche Produkte man schon vorher bei einem anderen Laden gekauft hat. Metro reagierte und bietet einen so genannten Deaktvierer, einen Zerstörer des Senders. Viele Kunden lassen es noch liegen und benutzen es nicht.

Das Chipsüberwachungssystem hat riesen Vorteile bei Lebensmittelsicherheit, Kühlüberwachung, Liefersicherheit. Das sind alle Dinge was für die Menschen zu Gute kommen.

2. Aufgabe

Adatvédelmi tudnivalók

Nagy örömmel fogadjuk az Ön látogatását a Web-lapunkon. Köszönjük Társaságunk, termékeink és Web-lapunk iránti érdeklődését.

Az Ön magánszférájának védelme a Web-lap használata során számunkra nagyon fontos, ezért kérjük vegye figyelembe a következő információkat:

Általános tudnivalók

Az ING-DiBa RT.a továbbiakban "ING-DiBa", az Interneten keresztül különböző pénzügyi banki és biztosítási termékeket kínál. Ügyfeleink ezenkivül kiegészítő szolgáltatásként az Internetbankot és a Brókercégünket is elérhetik.

Az ING-DiBa tisztában van az Ön bizalmas személyes adatainak jelentőségével. Biztosíthatjuk, hogy ügyfeleink és érdeklődőink által az Interneten megadott adatokat bizalmasan kezeljük.

Személyes adatok olyan adatok amelyek természetes személlyel kapcsolatba hozhatók. Ilyen adatok lehetnek pl.: a név, aláírás, telefonszám és más az üzletkötéshez szükséges adat. Olyan információ, amely nem hozható közvetlenül az Ön személyével kapcsolatba nem tartoznak hozzá.

Az ügyfelek és érdeklődők személyes adatait szigorú biztonsági követelményeknek vetjük alá a feldolgozás során, a visszaélések elkerülése érdekében.

Személyes adatok tárolása és feldolgozása

Személyes adatokat csak abban az esetben tárolunk, amennyiben Ön pl. egy szerződéskötéshez, vagy személyes szolgáltatások regisztrációjához ad meg.

Az adatokat a szolgáltatások, vagy pénzügyi tranzakciók teljesítéséhez használjuk fel. Amennyiben Ön hozzájárul, úgy a továbbiakban is informáljuk az ING-DiBa termékeiről.

Minden személyes adatot kódolt formában továbbítunk, annak érdekében, hogy az harmadik személy kezébe ne kerülhessen és visszaélésre ne adhasson okot.

Személyes adatok használata és továbbítása

Az ING-DiBa az Ön által megadott és tárolt adatokat csak a szerződés ügyviteli folyamatához, annak ellenőrzéséhez, ezen túlmenően reklám, vagy piac-, és véleménykutatás céljára használjuk fel. A reklám, piac-, és véleménykutatás miatti adathasználatot Ön bármikor lemondhatja. Az Ön adatainak a továbbítása törvényi kötelezettségünknek megfelelően csak az Ön hozzájárulásával történhet.

Az Ön jogai

Tájékoztatjuk minden olyan személyes adatról, amelyet tárolni fogunk. Ezen túlmenően nem tárolunk, nem használunk fel és nem dolgozunk fel az Ön hozzájárulása nélkül semmilyen személyes adatot. Jóváhagyását Ön bármikor töröltetheti.

Amennyiben Ön az általunk tárolt adatokkal nem ért egyet, vagy azok nem felelnek meg a valóságnak, akkor azokat a jogi előírásoknak megfelelően töröljük, zároljuk, vagy helyesbítjük.

Kívánságára az adatbázisunkban tárolt személyes adatairól informáljuk.

Amennyiben Ön az ING-DiBa ügyfele, úgy az adattárolás, adathasználat az Internetbank és és Brókercég keretein belül az Önnel kötött szerződésekre vonatkozóan hatályos.

Biztonsági technológiánk

A személyes adatokat tároló adatok 128 Bit-tel kódoltak és a nemzetközi tanúsítvánnyal hitelesítettek.

Az Internetbankra + Brókercégre vonatkozóan további biztonsági intézkedések vannak (DiBa Key / iTAN-technika).

Jogosulatlan hozzáférések egy tűzfal rendszeren keresztül blokkolva vannak.

További információkat Web-oldalunkon a "Biztonság" alatt találhat.

Amennyiben további kérdései vagy javaslatai vannak az adatvédelemmel kapcsolatban, úgy a datenschutz@ing-diba.de címen tud velünk kapcsolatot teremteni.

LITERATUR I.-II.-III.

VERWENDETE LITERATUR

http://de.wikipedia.org/wiki/Datenschutz

www.business-wissen.de

Customer Relationship Management strukturiert dargestellt: Prozesse, Systeme

szerző: Jörg Schumacher,Matthias Meyer, Springer 2003

Oliver Christ, Volker Bach : Contact Center - Organisationsmodelle und Systemarchitektur, Dissertation der Universität St. Gallen 2573

T. Schwarz: Leitfaden Dialogmarketing, Marketing-Börse 2008

Günter Greff: Erfolgreiches Telefonmarketing www.marketingbörse.de Fachartikel: 05.02.2009

Gaby S. Graupner: Typgerechtes Telefonieren/ Die Deutsche Akademie für Training, 2008

Greff G.: „Nie mehr Kaltanrufe". - Serie in www.Call-Center-Experts.de.

Barth F.: Telefonieren mit Erfolg: Die Kunst des richtigen Telefonmarketing / Deutscher Taschenbuch Verlag - 1. Januar 2001

Katja Hinzberg www.marketing-text.de/ 2009

A(z) 2569-06 modul n22-es szakmai tankönyvi tartalomeleme felhasználható az alábbi szakképesítésekhez:

A szakképesítés OKJ azonosító száma:	A szakképesítés megnevezése
52 347 03 0100 31 02	Telefonkezelő, ügyféltájékoztató
52 347 03 0100 52 01	Telemarketing asszisztens
52 347 02 0000 00 00	Személyes ügyfélszolgálati asszisztens
52 347 03 0000 00 00	Telefonos és elektronikus ügyfélkapcsolati asszisztens

A szakmai tankönyvi tartalomelem feldolgozásához ajánlott óraszám:
5 óra

A kiadvány az Új Magyarország Fejlesztési Terv
TÁMOP 2.2.1 08/1-2008-0002 „A képzés minőségének és tartalmának fejlesztése” keretében készült.
A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

Kiadja a Nemzeti Szakképzési és Felnőttképzési Intézet
1085 Budapest, Baross u. 52.
Telefon: (1) 210-1065, Fax: (1) 210-1063

Felelős kiadó:
Nagy László főigazgató